The Lang-Trotter Conjecture on Average

Stephan Baier

February 2, 2008

Abstract

For an elliptic curve E over $\mathbb{Q}$ and an integer r let $\pi_E^r(x)$ be the number of primes $p \le x$ of good reduction such that the trace of the Frobenius morphism of $E/\mathbb{F}_p$ equals r. We consider the quantity $\pi_E^r(x)$ on average over certain sets of elliptic curves. More in particular, we establish the following: If $A, B > x^{1/2+\varepsilon}$ and $AB > x^{3/2+\varepsilon}$, then the arithmetic mean of $\pi_E^r(x)$ over all elliptic curves $E : y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$, $|a| \le A$ and $|b| \le B$ is $\sim C_r \sqrt{x}/\log x$, where C_r is some constant depending on r. This improves a result of C. David and F. Pappalardi. Moreover, we establish an "almost-all" result on $\pi_E^r(x)$.

Mathematics Subject Classification (2000): 11G05

Keywords: Lang-Trotter conjecture, average Frobenius distribution, character sums

1 Introduction and main results

Let E be an elliptic curve over $\mathbb{Q}$. For any prime number p of good reduction, let $a_p(E)$ be the trace of the Frobenius morphism of $E/\mathbb{F}_p$. Then the number of points on the reduced curve modulo p equals $\#E(\mathbb{F}_p) = p + 1 - a_p(E)$. Furthermore, by Hasse's theorem, $|a_p(E)| \le 2\sqrt{p}$.

For a fixed integer r, let

$$\pi_E^r(x) := \#\{p \le x : a_p(E) = r\}.$$

If $r = 0$ and E has complex multiplication, Deuring [2] showed that

$$\pi_E^0(x) \sim \frac{\pi(x)}{2} \qquad \text{as } x \to \infty.$$

Primes p with $a_p = 0$ are known as "supersingular primes".

Lang and Trotter [7] conjectured that for all other cases an asymptotic estimate of the form

$$\pi_E^r(x) \sim C_{E,r} \cdot \frac{\sqrt{x}}{\log x} \qquad \text{as } x \to \infty$$

with a well-defined constant $C_{E,r} \geq 0$ holds. They used a probabilistic model to give an explicit description of the constant $C_{E,r}$. The constant can be 0, and the asymptotic estimate is then interpreted to mean that there is only a finite number of primes such that $a_p(E) = r$. A concise account of Lang-Trotter's probabilistic model and an expression of $C_{E,r}$ as an Euler product can be found in [1].

Fouvry and Murty [5] obtained average estimates related to the Lang-Trotter conjecture for the supersingular case $r = 0$. Their result was later generalized by David and Pappalardi [1] to any $r \in \mathbb{Z}$. In this paper, we shall improve the results of David and Pappalardi.

As in [1], we define

$$\pi_{1/2}(x) := \int\limits_2^x \frac{\mathrm{d}t}{2\sqrt{t}\log t} \sim \frac{\sqrt{x}}{\log x}$$

and a constant C_r by

$$C_r := \frac{2}{\pi} \prod_{l|r} \left(1 - \frac{1}{l^2}\right) \prod_{l\nmid r} \frac{l(l^2-l-1)}{(l-1)(l^2-1)}. \tag{1.1}$$

Our first result is

Theorem 1: *Let r be a fixed integer and $A, B \geq 1$. Then, for every $c > 0$, we have*

$$\begin{aligned}&\frac{1}{4AB} \sum_{|a|\leq A} \sum_{|b|\leq B} \pi_{E(a,b)}^r \\ = \;& C_r \pi_{1/2}(x) + O\left(\left(\frac{1}{A} + \frac{1}{B}\right) x \log x + \frac{x^{5/4}\log^3 x}{\sqrt{AB}} + \frac{\sqrt{x}}{\log^c x}\right),\end{aligned}$$

where the implied O-constant depends only on c and r.

David and Pappalardi [1] obtained the above result with $(1/A+1/B)x^{3/2}$ in place of $(1/A+1/B)x\log x$ and $x^{5/2}/(AB)$ in place of $x^{5/4}\log^3 x/\sqrt{AB}$ in the O-term.

From Theorem 1, we immediately obtain the following Lang-Trotter type estimate on average.

Theorem 2: *Let $\varepsilon>0$. If $A,B>x^{1/2+\varepsilon}$ and $AB>x^{3/2+\varepsilon}$, we have as $x\to\infty$,*

$$\frac{1}{4AB}\sum_{|a|\le A}\sum_{|b|\le B}\pi^r_{E(a,b)}\sim C_r\frac{\sqrt{x}}{\log x}. \tag{1.2}$$

In [1], (1.2) was proved under the stronger condition $A,B>x^{1+\varepsilon}$.

David and Pappalardi asked if (1.2) is consistent with the Lang-Trotter conjecture in the sense that

$$\frac{1}{4AB}\sum_{|a|\le A}\sum_{|b|\le B}C_{E(a,b),r}\sim C_r \tag{1.3}$$

as $A,B\to\infty$. N. Jones [6] proved that this average estimate holds if the summation is restricted to a,b such that $E(a,b)$ is a Serre curve. An elliptic curve is called a Serre curve if $\phi_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is an index two subgroup in $\mathrm{GL}_2(\hat{\mathbb{Z}})$, where $\phi_E:\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\mathrm{GL}_2(\hat{\mathbb{Z}})$ denotes the Galois representation associated to E. By a result of Serre [8], ϕ_E is never surjective, so in other words, E is a Serre curve if its Galois representation has "image as large as possible". Moreover, extending a result of W.D. Duke [3], Jones proved that, according to height, almost all elliptic curves over $\mathbb{Q}$ are Serre curves. This gives some evidence that (1.3) really holds.

Furthermore, David and Pappalardi proved that

$$\pi^r_{E(a,b)}(x)\sim C_r\sqrt{x}/\log x$$

holds for "almost all" curves $E(a,b)$ with $|a|\le A$ and $|b|\le B$ if $A,B>x^{2+\varepsilon}$ (Theorem 1.3. in [1]). Here we show that this "almost-all" result holds for considerably smaller A,B-ranges.

Theorem 3: *Let $\varepsilon > 0$ and fix $c > 0$. If $A, B > x^{1+\varepsilon}$ and $x^{3+\varepsilon} < AB < \exp(\exp(\sqrt{x}/\log^c x))$, then for all $d > 2c$ and for all elliptic curves $E(a,b)$ with $|a| \le A$ and $|b| \le B$ with at most $O(AB/\log^d z)$ exceptions, we have the inequality*

$$|\pi^r_{E(a,b)}(x) - C_r \pi_{1/2}(x)| \ll \frac{\sqrt{x}}{\log^c x}.$$

We shall establish the following more general estimate from which Theorem 3 can be derived by the Turán normal order method (*c.f.* [1]).

Theorem 4: *Let $\varepsilon > 0$. If $A, B > x^{1/2+\varepsilon}$ and $AB > x^{3/2+\varepsilon}$, then for every $c > 0$, we have*

$$(1.4) \qquad \frac{1}{4AB} \sum_{|a| \le A} \sum_{|b| \le B} \left| \pi^r_{E(a,b)}(x) - C_r \pi_{1/2}(x) \right|^2$$
$$= O\left(\left(\frac{1}{A} + \frac{1}{B} \right) x^2 + \frac{x^{5/2} \log^3 x}{\sqrt{AB}} + \frac{x}{\log^c x} + x^{1/2} \log\log(10AB) \right),$$

where the implied O-constant depends only on c and r.

2 The work of David-Pappalardi

The following observations are the starting point of David-Pappalardi's work in [1].

Lemma 1: *For $r \le 2\sqrt{p}$, the number of $\mathbb{F}_p$-isomorphism classes of elliptic curves over $\mathbb{F}_p$ with $p+1-r$ points is the total number of ideal classes of the ring $\mathbb{Z}[(D+\sqrt{D})/2]$, where $D = r^2 - 4p$ is a negative integer which is congruent to 0 or 1 modulo 4. This number is the Kronecker class number $H(r^2 - 4p)$.*

In the following, we set $H_{r,p} = H(r^2 - 4p)$.

Lemma 2: *Suppose that $p \ne 2, 3$. Then any elliptic curve over $\mathbb{F}_p$ has a model*

$$E \ : \ Y^2 = X^3 + aX + b$$

with $a, b \in \mathbb{F}_p$. The elliptic curves $E'(a', b')$ over p, which are $\mathbb{F}_p$-isomorphic to E, are given by all the choices

$$a' = \mu^4 a \quad \text{and} \quad b' = \mu^6 b$$

with $\mu \in \mathbb{F}_p^*$. The number of such E' is

$$\begin{array}{ll} (p-1)/6, & \text{if } a = 0 \text{ and } p \equiv 1 \bmod 3; \\ (p-1)/4, & \text{if } b = 0 \text{ and } p \equiv 1 \bmod 4; \\ (p-1)/2, & \text{otherwise.} \end{array}$$

The above Lemmas 1 and 2 imply that the number of curves $E(a, b)$ with $a, b \in \mathbb{Z}$, $0 \le a, b < p$ and $a_p(E(a, b)) = r$ is

$$\frac{pH_{r,p}}{2} + O(p). \tag{2.1}$$

Now David and Pappalardi [1] write

$$\begin{aligned} &\frac{1}{4AB} \sum_{|a| \le A} \sum_{|b| \le B} \pi^r_{E(a,b)}(x) \\ = \ &\frac{1}{4AB} \sum_{B(r) < p \le x} \sharp\{|a| \le A, \ |b| \le B \ : \ a_p(E(a, b)) = r\}, \end{aligned} \tag{2.2}$$

where $B(r) = \max\{3, r, r^2/4\}$. Using (2.1), the term on the right-hand side is

$$\frac{1}{4AB} \sum_{B(r) < p \le x} \left(\frac{2A}{p} + O(1) \right) \left(\frac{2B}{p} + O(1) \right) \left(\frac{pH_{r,p}}{2} + O(p) \right). \tag{2.3}$$

This asymptotic estimate was used by David and Pappalardi to prove their main theorem on the average Frobenius distribution of elliptic curves (Theorem 1 in [1]). For the main term in (2.3) David and Pappalardi proved the following.

Lemma 3: *Let r be a fixed integer. Then, for every $c > 0$, we have*

$$\sum_{B(r) < p \le x} \frac{H_{r,p}}{2p} = C_r \pi_{1/2}(x) + O\left(\frac{\sqrt{x}}{\log^c x} \right),$$

where the constant C_r is defined as in (1.1) and the implied O-constant depends only on r and c.

In this paper we shall sharpen the error term in (2.3).

3 Preliminaries

We first characterize the elliptic curves lying in a fixed $\mathbb{F}_p$-isomorphism class, where p is a prime $\neq 2, 3$. In the following, for $z \in \mathbb{Z}$ let $\overline{z}$ be the reduction of z mod p. Furthermore, let z^{-1} be a multiplicative inverse mod p, that is, $zz^{-1} \equiv 1 \bmod p$.

Lemma 4: *Let $a, b, c, d \in \mathbb{Z}$, $p \nmid abcd$ and E_1, E_2 be elliptic curves over $\mathbb{F}_p$ given by*

$$E_1 \ : \ Y^2 = X^3 + \overline{a}X + \overline{b}.$$

and

$$E_2 \ : \ Y^2 = X^3 + \overline{c}X + \overline{d}.$$

(i) *If $p \equiv 1 \bmod 4$, then E_1 and E_2 are $\mathbb{F}_p$-isomorphic if and only if ca^{-1} is a biquadratic residue mod p and $c^3a^{-3} \equiv d^2b^{-2} \bmod p$.*

(ii): *If $p \equiv 3 \bmod 4$, then E_1 and E_2 are $\mathbb{F}_p$-isomorphic if and only if ca^{-1} and db^{-1} are quadratic residues mod p and $c^3a^{-3} \equiv d^2b^{-2} \bmod p$.*

Proof: By Lemma 2, the curves E_1 and E_2 are $\mathbb{F}_p$-isomorphic if and only if there exists an integer m such that $p \nmid m$ and

$$c \equiv m^4 a \bmod p \quad \text{and} \quad d \equiv m^6 b \bmod p. \tag{3.1}$$

(i) Suppose that $p \equiv 1 \bmod 4$. If (3.1) is satisfied, then it follows that ca^{-1} is a biquadratic residue mod p and $c^3a^{-3} \equiv m^{12} \equiv d^2b^{-2} \bmod p$.

Assume, conversely, that ca^{-1} is a biquadratic residue mod p and

$$c^3a^{-3} \equiv d^2b^{-2} \bmod p. \tag{3.2}$$

Since $p \equiv 1 \bmod 4$, there exist two solutions m_1, m_2 of the congruence $c \equiv m^4a \bmod p$ such that $m_2^2 \equiv -m_1^2 \bmod p$, and (3.2) implies that $d^2b^{-2} \equiv m_j^{12} \bmod p$ for $j = 1, 2$. From this it follows that $db^{-1} \equiv m_1^6 \bmod p$ or $db^{-1} \equiv$

$-m_1^6 \equiv m_2^6 \bmod p$. Hence, the system (3.1) is soluble for m. This completes the proof of **(i)**.□

(ii) Suppose that $p \equiv 3 \bmod 4$. If (3.1) is satisfied, then it follows that ca^{-1} and db^{-1} are quadratic residues mod p and $c^3a^{-3} \equiv m^{12} \equiv d^2b^{-2} \bmod p$.

Assume, conversely, that ca^{-1} and db^{-1} are quadratic residues mod p and (3.2) is satisfied. Then, since $p \equiv 3 \bmod 4$, ca^{-1} is also a biqadratic residue. Hence, there exists a solution m of the congruence $c \equiv m^4a \bmod p$. Further, (3.2) implies that $d^2b^{-2} \equiv m^{12} \bmod p$. From this it follows that that $db^{-1} \equiv m^6 \bmod p$ or $db^{-1} \equiv -m^6 \bmod p$. But $-m^6$ is a quadratic non-residue mod p since $p \equiv 3 \bmod 4$. Thus $db^{-1} \not\equiv -m^6 \bmod p$ since db^{-1} is supposed to be a quadratic residue mod p. Hence, we have $db^{-1} \equiv m^6 \bmod p$, and so the system (3.1) is soluble for m. This completes the proof of **(ii)**.□

We shall detect elliptic curves lying in a fixed $\mathbb{F}_p$-isomorphism class by using Dirichlet characters. For the estimation of certain error terms we then need the following results on character sums.

Lemma 5: *Let $q, N \in \mathbb{N}$ and (a_n) be any sequence of complex numbers. Then*

$$\sum_{\chi \bmod q} \left| \sum_{n \le N} a_n \chi(n) \right|^2 = \varphi(q) \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left| \sum_{\substack{n \le N \\ n \equiv a \bmod q}} a_n \right|^2,$$

where the outer sum on the left-hand side runs over all Dirichlet characters mod q.

Proof: This is a consequence of the orthogonality relations for Dirichlet characters. □

Lemma 6: *Let $q, N \in \mathbb{N}$, $q \ge 2$. Then*

$$\sum_{\chi \ne \chi_0} \left| \sum_{n \le N} \chi(n) \right|^4 \ll N^2 q \log^6 q,$$

where the outer sum on the left-hand side runs over all non-principal Dirichlet characters mod q.

Proof: This is Lemma 3 in [4]. $\square$

Lemma 7: *Let $q, N \in \mathbb{N}$, $q \geq 2$ and χ be any non-principal character mod q. Then*

$$\sum_{n \leq N} \chi(n) \ll \sqrt{q} \log q.$$

Proof: This is the well-known inequality of Polya-Vinogradov. $\square$

Furthermore, we shall need the following estimates for sums over $H_{r,p}$.

Lemma 8: *We have*

$$\sum_{B(r)<p\leq x} H_{r,p}^{1/2} \ll x^{5/4}, \qquad \sum_{B(r)<p\leq x} \frac{H_{r,p}}{\sqrt{p}} \ll x, \qquad \sum_{B(r)<p\leq x} \frac{H_{r,p}}{p} \ll \sqrt{x}$$

and

$$\sum_{B(r)<p\leq x} \frac{H_{r,p}}{p^2} \ll 1.$$

Proof: By (26) in [1], we have

$$\sum_{B(r)<p\leq x} H_{r,p} \ll x^{3/2}. \tag{3.3}$$

Using the Cauchy-Schwarz inequality, we obtain

$$\sum_{B(r)<p\leq x} H_{r,p}^{1/2} \ll x^{1/2} \left(\sum_{B(r)<p\leq x} H_{r,p} \right)^{1/2} \ll x^{5/4}$$

from (3.3). The remaining three estimates in Lemma 8 can be derived from (3.3) by partial summation.$\square$

Finally, we shall need the following bound.

Lemma 9: The number of $\mathbb{F}_p$-isomorphism classes of elliptic curves containing curves

$$E \ : \ Y^2 = X^3 + aX + b$$

over $\mathbb{F}_p$ with $a=0$ or $b=0$ is bounded by 10.

Proof: By Lemma 2, the number of $\mathbb{F}_p$-isomorphism classes containing curves $E(0,b)$ with $b\in\mathbb{F}_p^*$ is ≤ 6, and the number of $\mathbb{F}_p$-isomorphism classes containing curves $E(a,0)$ with $a\in\mathbb{F}_p^*$ is ≤ 4. $\Box$

4 Proof of Theorem 1

Let $I_{r,p}$ be the number of $\mathbb{F}_p$-isomorphism classes of elliptic curves

$$E\ :\ Y^2=X^3+cX+d$$

over $\mathbb{F}_p$ with $p+1-r$ points such that $c,d\ne 0$. Let $(u_{p,j},v_{p,j})$, $j=1,...,I_{r,p}$ be pairs of integers such that the curves $E(\overline{u_{p,j}},\overline{v_{p,j}})$ form a system of representatives of these isomophism classes. We now write

$$\begin{aligned} & \sharp\{|a|\le A,\ |b|\le B\ :\ a_p(E(a,b))=r\} \\ = & \sharp\{|a|\le A,\ |b|\le B\ :\ p\nmid ab,\ a_p(E(a,b))=r\}+ \\ & O\left(\frac{AB}{p}+A+B\right) \end{aligned}$$

and

$$\begin{aligned} & \sharp\{|a|\le A,\ |b|\le B\ :\ p\dagger ab,\ a_p(E(a,b))=r\} \\ = & \sum_{j=1}^{I_{r,p}}\sharp\{|a|\le A,\ |b|\le B\ : E(\overline{a},\overline{b})\cong E(\overline{u_{p,j}},\overline{v_{p,j}})\}, \end{aligned} \tag{4.1}$$

where the symbol $\cong$ stands for "$\mathbb{F}_p$-isomorphic". We rewrite the term on the right-hand side of (4.1) as a character sum. If $p\equiv 1 \bmod 4$, then, by Lemma 4(i) and the character relations, this term equals

$$\frac{1}{4\varphi(p)}\sum_{j=1}^{I_{r,p}}\sum_{|a|\le A}\sum_{|b|\le B}\sum_{k=1}^{4}\left(\frac{au_{p,j}^{-1}}{p}\right)_4^k\sum_{\chi \bmod p}\chi(a^3u_{p,j}^{-3}b^{-2}v_{p,j}^2), \tag{4.2}$$

where $(\cdot/p)_4$ is the biquadratic residue symbol. If $p\equiv 3 \bmod 4$, then, by Lemma 4(ii) and the character relations, the term on the right-hand side of

(4.1) equals

$$\frac{1}{4\varphi(p)}\sum_{j=1}^{I_{r,p}}\sum_{|a|\le A}\sum_{|b|\le B}\left(\chi_0(a)+\left(\frac{au_{p,j}^{-1}}{p}\right)\right)\left(\chi_0(b)+\left(\frac{bv_{p,j}^{-1}}{p}\right)\right)$$
$$\sum_{\chi \bmod p}\chi(a^3u_{p,j}^{-3}b^{-2}v_{p,j}^2),$$

where $(\cdot/p)$ is the Legendre symbol and χ_0 is the principal character.

In the following, we consider only the case $p\equiv 1 \bmod 4$. The case $p\equiv 3 \bmod 4$ can be treated in a similar way. The expression in (4.2) equals

$$\frac{1}{4\varphi(p)}\sum_{k=1}^{4}\sum_{\chi \bmod p}\sum_{j=1}^{I_{r,p}}\left(\frac{u_{p,j}}{p}\right)_4^{-k}\overline{\chi}^3(u_{p,j})\chi^2(v_{p,j})\sum_{|a|\le A}\left(\frac{a}{p}\right)_4^{k}\chi^3(a)\sum_{|b|\le B}\overline{\chi}^2(b).$$

We split this expression into 3 parts M, E_1, E_2, where

(**i**) M = contribution of k,χ with $(\cdot/p)_4^k\chi^3=\chi_0$, $\chi^2=\chi_0$;

(**ii**) E_1 = contribution of k,χ with $(\cdot/p)_4^k\chi^3\ne\chi_0$, $\chi^2=\chi_0$ or $(\cdot/p)_4^k\chi^3=\chi_0$, $\chi^2\ne\chi_0$;

(**iii**) E_2 = contribution of k,χ with $(\cdot/p)_4^k\chi^3\ne\chi_0$, $\chi^2\ne\chi_0$.

As one may expect, M shall turn out to be the main term and E_1, E_2 to be the error terms.

Estimation of M. The only cases in which $(\cdot/p)_4^k\chi^3=\chi_0$ and $\chi^2=\chi_0$ are $k=0$, $\chi=\chi_0$ and $k=2$, $\chi=(\cdot/p)$. Now, by a short calculation, we obtain

$$M=\frac{ABI_{r,p}}{2p}\left(1+O\left(\frac{1}{p}\right)\right). \tag{4.3}$$

By Lemma 9, we have $H_{r,p}-I_{r,p}\le 10$. Combining this with (4.3), we obtain

$$M=\frac{ABH_{r,p}}{2p}+O\left(\frac{AB}{p}+\frac{ABH_{r,p}}{p^2}\right).$$

Estimation of E_1. The number of solutions (k,χ) with $k=1,...,4$ of $(\cdot/p)_4^k\chi^3=\chi_0$ is bounded by 12, and $\chi^2=\chi_0$ has precisely 2 solutions χ. Thus E_1 is the sum of at most $12+4\cdot 2=20$ terms of the form

$$\frac{1}{4\varphi(p)}\sum_{j=1}^{I_{r,p}}\overline{\chi_1}(u_{p,j})\overline{\chi_2}(v_{p,j})\sum_{|a|\le A}\chi_1(a)\sum_{|b|\le B}\chi_2(b),$$

where exactly one of the characters χ_1, χ_2 is the principal character χ_0. Therefore, Lemma 7 implies that

$$E_1 \ll \frac{I_{r,p}(A+B)}{\sqrt{p}}\log p.$$

Estimation of E_2. Given $k\in\mathbb{Z}$ and a character χ_1 mod p, the number of solutions χ of $\left(\frac{\cdot}{p}\right)_4^k\chi^{-3}=\chi_1$ is ≤ 3, and the number of solutions χ of $\chi^2=\chi_1$ is ≤ 2. Thus, using the Cauchy-Schwarz inequality, we deduce that

$$E_2 \ll \frac{1}{p}\sum_{k=1}^{4}\left(\sum_{\chi}\left|\sum_{j=1}^{I_{r,p}}\left(\frac{u_{p,j}}{p}\right)_4^k\chi(u_{p,j}^{-3}v_{p,j}^2)\right|^2\right)^{1/2}\times \left(\sum_{\chi\ne\chi_0}\left|\sum_{|a|\le A}\chi(a)\right|^4\right)^{1/4}\left(\sum_{\chi\ne\chi_0}\left|\sum_{|b|\le B}\chi(b)\right|^4\right)^{1/4}. \tag{4.4}$$

By Lemma 4(i), the number of j's such that $u_{p,j}^{-3}v_{p,j}^2$ lie in a fixed residue class mod p is bounded by 4. Using this, Lemma 5 and Lemma 6, the expression on the right-hand side of (4.4) is dominated by

$$\ll (I_{r,p}AB)^{1/2}\log^3 p.$$

The final estimate. Combining all contributions, and using $I_{r,p}\le H_{r,p}$, we obtain

$$\begin{aligned}&\sharp\{|a|\le A,\ |b|\le B\ :\ a_p(E(a,b))=r\}\\ &= \frac{ABH_{r,p}}{2p}+O\left(\frac{AB}{p}+\frac{ABH_{r,p}}{p^2}+A+B+(H_{r,p}AB)^{1/2}\log^3 p+\right.\\ &\qquad\left.\frac{H_{r,p}(A+B)}{\sqrt{p}}\log p\right)\end{aligned} \tag{4.5}$$

The result of Theorem 1 now follows from (2.2), (4.5), Lemma 3 and Lemma 8.

5 Proof of Theorem 4

As in [1], we set

$$\mu := \frac{1}{4AB} \sum_{|a|\le A} \sum_{|b|\le B} \pi^r_{E(a,b)}(x).$$

Fix any $c > 0$. Using Theorem 1 and following the arguments in [1], if $A, B > x^{1/2+\varepsilon}$ and $AB > x^{3/2+\varepsilon}$, then

$$\mu = C_r \pi_{1/2}(x) + O\left(\frac{\sqrt{x}}{\log^c x}\right), \tag{5.1}$$

and the left-hand side of (1.4) is

$$\ll \left| \sum_{|a|\le A} \sum_{|b|\le B} \sharp\{p, q \le x \ : \ p \ne q,\ a_p(E(a,b)) = r = a_q(E(a,b))\} \ - \mu^2 \right| + \mu + \frac{x}{\log^{2c} x}, \tag{5.2}$$

where p, q denote primes. Similarly as in the preceeding section, we have

$$\begin{aligned} &\sum_{|a|\le A} \sum_{|b|\le B} \sharp\{p, q \le x \ : \ p \ne q,\ a_p(E(a,b)) = r = a_q(E(a,b))\} \\ &= \sum_{\substack{B(r)<p,q\le x \\ p\ne q}} \sharp\{|a| \le A,\ |b| \le B \ : \ a_p(E(a,b)) = r = a_q(E(a,b))\}. \end{aligned} \tag{5.3}$$

Using Theorem 1 and $\sharp\{p\ :\ p|ab\} = \omega(|ab|) \ll \log\log(10|ab|)$ if $ab \neq 0$, we deduce

$$
\begin{aligned}
(5.4)\quad & \sum_{\substack{B(r)<p,q\le x\\ p\neq q}} \sharp\{|a|\le A,\ |b|\le B\ :\ a_p(E(a,b))=r=a_q(E(a,b))\}\\
= & \sum_{\substack{B(r)<p,q\le x\\ p\neq q}} \sharp\{|a|\le A,\ |b|\le B\ :\ p,q\nmid ab,\ a_p(E(a,b))=r=a_q(E(a,b))\}\\
& +O\left(\sum_{p\le x}\ \sum_{\substack{|a|\le A,\ |b|\le B\\ p|ab}} \pi^r_{E(a,b)}(x)\right)\\
= & \sum_{\substack{B(r)<p,q\le x\\ p\neq q}} \sharp\{|a|\le A,\ |b|\le B\ :\ p,q\nmid ab,\ a_p(E(a,b))=r=a_q(E(a,b))\}\\
& +O\left(ABx^{1/2}\log\log(10AB)+(A+B)x^{3/2}\right).
\end{aligned}
$$

Now we fix p,q with $p \neq q$. In the following, we confine ourselves to the case when $p \equiv q \equiv 1 \bmod 4$. The remaining cases $pq \equiv -1 \bmod 4$ and $p \equiv q \equiv 3 \bmod 4$ can be treated in a similar way. Similarly as in the preceeding section, we can express the term

$$\sharp\{|a|\le A,\ |b|\le B\ :\ p,q\nmid ab,\ a_p(E(a,b))=r=a_q(E(a,b))\}$$

as a character sum

$$
\begin{aligned}
&\frac{1}{16\varphi(p)\varphi(q)}\sum_{i=1}^{I_{r,p}}\sum_{j=1}^{I_{r,q}}\sum_{|a|\le A}\sum_{|b|\le B}\sum_{k=1}^{4}\left(\frac{au_{p,i}^{-1}}{p}\right)_4^k \sum_{\chi \bmod p}\chi(a^3u_{p,i}^{-3}b^{-2}v_{p,i}^2)\\
&\sum_{l=1}^{4}\left(\frac{au_{q,j}^{-1}}{q}\right)_4^l \sum_{\chi' \bmod q}\chi'(a^3u_{q,j}^{-3}b^{-2}v_{q,j}^2).
\end{aligned}
$$

This sum equals

$$(5.5)\quad \frac{1}{16\varphi(p)\varphi(q)} \sum_{k=1}^{4}\sum_{l=1}^{4} \sum_{\chi \bmod p} \sum_{\chi' \bmod q} \left(\sum_{i=1}^{I_{r,p}} \left(\frac{u_{p,i}}{p}\right)_4^{-k} \overline{\chi}^3(u_{p,i})\chi^2(v_{p,i}) \right) \times$$
$$\left(\sum_{j=1}^{I_{r,q}} \left(\frac{u_{q,j}}{q}\right)_4^{-l} \overline{\chi'}^3(u_{q,j}){\chi'}^2(v_{q,j}) \right) \left(\sum_{|a|\le A} \left(\frac{a}{p}\right)_4^{k} \left(\frac{a}{q}\right)_4^{l} (\chi\chi')^3(a) \right) \times$$
$$\left(\sum_{|b|\le B} \left(\overline{\chi\chi'}\right)^2(b) \right).$$

Let χ_0 be the principal character mod p and χ_0' be the principal character mod q. Then $\chi_0\chi_0'$ is the principal character mod pq. As previously, we split the expression in (5.5) into 3 parts M, E_1, E_2, where

(**i**) M = contribution of k, l, χ, χ' with
$(\cdot/p)_4^k(\cdot/q)_4^l(\chi\chi')^3 = \chi_0\chi_0'$, $(\chi\chi')^2 = \chi_0\chi_0'$;

(**ii**) E_1 = contribution of k, l, χ, χ' with
$(\cdot/p)_4^k(\cdot/q)_4^l(\chi\chi')^3 \neq \chi_0\chi_0'$, $(\chi\chi')^2 = \chi_0\chi_0'$ or
$(\cdot/p)_4^k(\cdot/q)_4^l(\chi\chi')^3 = \chi_0\chi_0'$, $(\chi\chi')^2 \neq \chi_0\chi_0'$;

(**iii**) E_2 = contribution of k, l, χ, χ' with
$(\cdot/p)_4^k(\cdot/q)_4^l(\chi\chi')^3 \neq \chi_0\chi_0'$, $(\chi\chi')^2 \neq \chi_0\chi_0'$.

Estimation of M. The only cases in which $(\cdot/p)_4^k(\cdot/q)_4^l(\chi\chi')^3 = \chi_0\chi_0'$, $(\chi\chi')^2 = \chi_0\chi_0'$ are:

(a) $k = l = 0$, $\chi = \chi_0$, $\chi' = \chi_0'$;

(b) $k = l = 2$, $\chi = (\cdot/p)$, $\chi' = (\cdot/q)$;

(c) $k = 0$, $l = 2$, $\chi = \chi_0$, $\chi' = (\cdot/q)$;

(d) $k = 2$, $l = 0$, $\chi = (\cdot/p)$, $\chi' = \chi_0$.

Now, by a short calculation, we obtain

$$(5.6)\qquad M = \frac{ABI_{r,p}I_{r,q}}{4pq}\left(1 + O\left(\frac{1}{p} + \frac{1}{q}\right)\right).$$

By Lemma 9, we have $H_{r,p} - I_{r,p} \leq 10$ and $H_{r,q} - I_{r,q} \leq 10$. Combining this with (5.6), we obtain

$$M = \frac{ABH_{r,p}H_{r,q}}{4pq} + O\left(\frac{AB(H_{r,p}+H_{r,q})}{pq} + ABH_{r,p}H_{r,q}\left(\frac{1}{p^2q} + \frac{1}{pq^2}\right)\right).$$

Estimation of E_1. The number of solutions (k,l,χ,χ') with $k,l = 1,...,4$ of $(\cdot/p)_4^k(\cdot/q)_4^l(\chi\chi')^3 \neq \chi_0\chi_0'$ is bounded by 12^2, and $(\chi\chi')^2 = \chi_0\chi_0'$ has precisely 4 solutions (χ,χ'). Thus E_1 is the sum of at most $144 + 16\cdot 4 = 228$ terms of the form

$$\frac{1}{16\varphi(p)\varphi(q)} \sum_{|a|\leq A} \chi_1(a) \sum_{|b|\leq B} \chi_2(b) \sum_{i=1}^{I_{r,p}} \chi_3(u_{p,i})\chi_4(v_{p,i}) \sum_{j=1}^{I_{r,q}} \chi_3'(u_{q,j})\chi_4'(v_{q,j}),$$

where χ_1, χ_2 are characters mod pq such that exactly one of them is the principal character, χ_3, χ_4 are characters mod p, and χ_3', χ_4' are characters mod q. Here the characters $\chi_{3,4}$, $\chi_{3,4}'$ depend on the characters $\chi_{1,2}$. Now Lemma 7 implies that

$$E_1 \ll \frac{I_{r,p}I_{r,q}(A+B)}{\sqrt{pq}} \log pq.$$

Estimation of E_2. Given $k,l \in \mathbb{Z}$ and a character χ_1 mod pq, the number of characters χ mod pq such that $(\cdot/p)_4^k(\cdot/q)_4^l(\chi\chi')^3 = \chi_1$ is ≤ 9, and the number of χ mod pq such that $\chi^2 = \chi_1$ is ≤ 4. Thus, using the Cauchy-Schwarz inequality, we deduce that

(5.7)

$$\begin{aligned} E_2 \quad \ll \quad & \frac{1}{pq}\sum_{k=1}^{4}\sum_{l=1}^{4}\left(\sum_{\chi}\left|\sum_{i=1}^{I_{r,p}}\left(\frac{u_{p,i}}{p}\right)_4^k \chi(u_{p,i}^{-3}v_{p,i}^2)\right|^2\right)^{1/2} \times \\ & \left(\sum_{\chi'}\left|\sum_{j=1}^{I_{r,q}}\left(\frac{u_{q,j}}{q}\right)_4^l \chi'(u_{q,j}^{-3}v_{q,j}^2)\right|^2\right)^{1/2} \left(\sum_{\chi_1\neq\chi_0\chi_0'}\left|\sum_{|a|\leq A}\chi_1(a)\right|^4\right)^{1/4} \\ & \left(\sum_{\chi_2\neq\chi_0\chi_0'}\left|\sum_{|b|\leq B}\chi(b)\right|^4\right)^{1/4}, \end{aligned}$$

where χ runs over all characters mod p, χ' runs over all characters mod q, and χ_1, χ_2 run over all non-principal characters mod pq.

By Lemma 4(i), the number of i's such that $u_{p,i}^{-3}v_{p,i}^2$ lie in a fixed residue class mod p is bounded by 4. The same is true for the number of $j's$ such that $u_{q,j}^{-3}v_{q,j}^2$ lie in a fixed residue class mod q. Using this, Lemma 5 and Lemma 6, the expression on the right-hand side of (5.7) is dominated by

$$\ll (I_{r,p}I_{r,q}AB)^{1/2}\log^3 pq.$$

The final estimate. Combining all contributions, and using $I_{r,p} \le H_{r,p}$, we obtain

$$\begin{aligned} &\sharp\{|a| \le A,\ |b| \le B\ :\ p,q \nmid ab,\ a_p(E(a,b)) = r = a_q(E(a,b))\} \\ = &\ \frac{ABH_{r,p}H_{r,q}}{4pq} + O\left(\frac{AB(H_{r,p}+H_{r,q})}{pq} + ABH_{r,p}H_{r,q}\left(\frac{1}{p^2q}+\frac{1}{pq^2}\right)\right. \\ &\left. + (H_{r,p}H_{r,q}AB)^{1/2}\log^3 pq + \frac{H_{r,p}H_{r,q}(A+B)}{\sqrt{pq}}\log pq\right). \end{aligned} \tag{5.8}$$

We have proved this estimate only for distinct primes p, q with $p \equiv q \equiv 1 \bmod 4$, but the same estimate can be proved for $pq \equiv -1 \bmod 4$ and $p \equiv q \equiv 3 \bmod 4$ in a similar way. Now, from (5.4), (5.8), Lemma 3 and Lemma 8, we obtain

$$\begin{aligned} &\frac{1}{4AB}\sum_{\substack{B(r)<p,q\le x\\ p\ne q}} \sharp\{|a| \le A,\ |b| \le B\ :\ a_p(E(a,b)) = r = a_q(E(a,b))\} \\ = &\ (C_r\pi_{1/2}(x))^2 + O\left(\sum_{B(r)<p\le x}\frac{H_{r,p}^2}{p^2} + \frac{x}{\log^c x} + x^{1/2}\log\log(10AB)\right. \\ &\left. + \frac{x^{5/2}}{\sqrt{AB}}\log^3 x + \left(\frac{1}{A}+\frac{1}{B}\right)x^2\right). \end{aligned} \tag{5.9}$$

From (23) in [1] and $h(d) \ll \sqrt{|d|}$, we obtain $H_{r,p} \ll p^{1/2+\varepsilon}$ which implies that

$$\sum_{B(r)<p\le x}\frac{H_{r,p}^2}{p^2} \ll x^{\varepsilon}. \tag{5.10}$$

The result of Theorem 4 now follows from (5.1), (5.2), (5.3), (5.9) and (5.10).

Acknowledgement. This paper was written when the author held a post-doctoral fellowship at the Queen's University in Kingston, Canada. The author wishes to thank this institution for financial support. He would further like to thank Prof. Ram Murty for his useful comments.

References

[1] C. David, F. Pappalardi, *Average Frobenius Distributions of Elliptic Curves*, Int. Math. Res. Not. (1999) 165-183.

[2] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. 14 (1941) 197-272.

[3] W.D. Duke, *Elliptic curves with no exceptional primes*, C. R. Acad. Sci., Paris, Sr. I, Math. 325 (1997) 813-818.

[4] J. Friedlander, H. Iwaniec, *The divisor problem for arithmetic progressions*, Acta Arith. 45 (1985) 273-277.

[5] E. Fouvry, M.R. Murty, *On the distribution of supersingular primes*, Canad. J. Math. 48 (1996) 81-104.

[6] N. Jones, *The constants in the Lang-Trotter conjecture*, preprint (2006).

[7] S. Lang, H. Trotter, *Frobenius Distributions in GL_2 extensions*, Lecture Notes in Math. 504 (1976) Springer-Verlag, Berlin.

[8] J. P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972) 259-331.

Address of the author:

Stephan Baier
Queen's University

Jeffery Hall
University Ave
Kingston, ON K7L3N6 Canada

e-mail: sbaier@mast.queensu.ca